

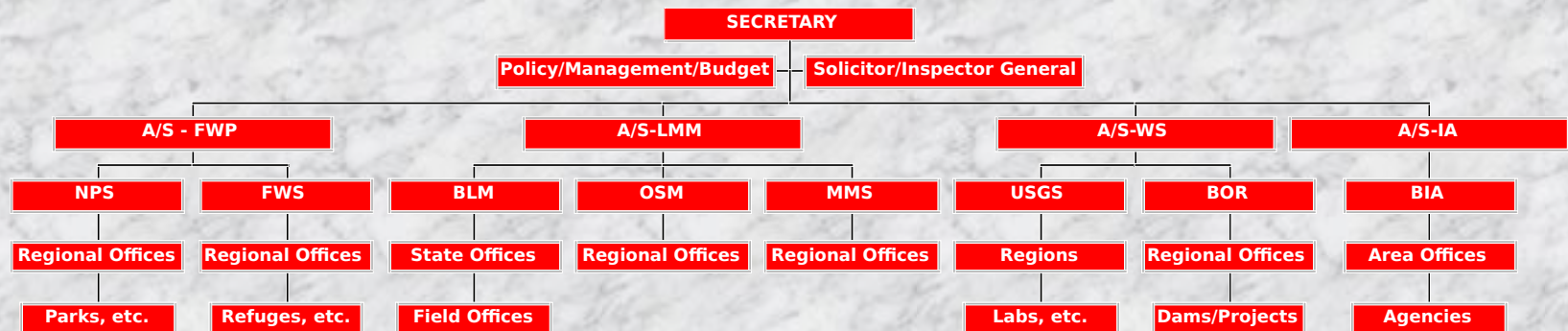
Y2K Planning & Preparedness in the Department of the Interior

Presentation to the Year 2000
Committee of the CIO
Council

February 25, 1999

*Jim Douglas
Emergency Coordinator
Office of Managing Risk and
Public Safety*

Overview of the Department of the Interior



Office of Managin
Richard B. L...

Introduction

- System Contingency Planning v. Continuity of Operations (COO) Planning
- Overview of COO Planning in DOI
- Day One Planning Approach

Contingency Planning for Systems

- Alternatives to use of automated systems, equipment
 - E.g. use of paper forms, accumulate data for later input, default actions

Business Contingency Planning

- **(Continuity of Operations)** Ensuring ability to perform essential [business] activities and functions - within an acceptable period of interruption
- May include and depend upon system contingency plans if those systems required for essential business activities and functions

Continuity of Operations Planning

■ Department Guidance

- *MRPS Policy Bulletin 98-001* (March 1998)

■ Presidential Guidance

- *Executive Order 12656* (1988)
- *Presidential Decision Directive 67* (October 1998)

Scope of COO Planning

- All facilities/locations
- All hazards/risks (natural, technological, human caused)
- With/without warning
- Acceptable level of interruption

Standard Elements

- Threat/Risk Assessment
- Determination of Essential Functions/Activities
- Relocation Sites
- Emergency Organization
- Alternate Communications (voice, data)
- Vital Records, Systems, and Equipment

- Communications Plan
 - Management
 - Employees
 - Public/Media
 - Partners/Stakeholders/Customers
- Testing/Exercising

Mission Essential Facilities

Mission Essential Facilities (MEF) are those facilities that (in association with organizations, personnel, and systems) are absolutely required in order to provide the inputs and outputs necessary to support the core processes, essential to accomplishing the Department's core mission as it relates to national security, national economic security, or continuity of government services.

Purpose

- Ensure that the most important facilities of the Department are identified and receive priority management attention in planning, testing, exercising, and oversight
- Ensure Y2K Readiness
- Ongoing COO capability to meet National guidance and standards

Examples

- Headquarters Offices
- Regional Offices
- Finance/Administrative/IRM Centers
- Key dams, power facilities, laboratories
- Major Wildland Fire Coordination Centers

Certification of Viable COO Capability

- Statement by each bureau director that COO plans (or equivalent) meeting Departmental standards has been developed
- Provides assurances to Departmental management
- Provides for accountability

Relating COO and Y2K Preparedness

- Y2K is a potential threat to ability to continue essential business functions (just like a hurricane, a flood, a bomb, a WMD)
- We know some things: When, What, How (maybe)
- But it is different: Technological, Systemic, Worldwide, Infrastructure Loss (potential)

DOI's Approach

- Treat Y2K as a special case for COO Planning
- Special annexes or supplementary plans
 - Day One Plan

Day One Planning in DOI

- Department-level Plan
 - Overall approach, architecture
 - Blend COO and Y2K information issues
- Bureau Plans
 - Support the Department's Plan
- Issues for Discussion/Consideration

Purpose/Goals of Day One Plan

- Ensure efficient flow of accurate information about status and condition of DOI facilities and systems during the transition from 1999 to 2000
- Monitor status of national and international conditions during the 1999-2000 transition as those conditions may affect the ability of the Department of the Interior to conduct essential activities and functions

- Coordinate federal activities or initiatives to address negative consequences resulting from the transition from 1999 to 2000
- Provide a safe, secure, and functional environment to perform required activities and functions
- Provide support to our international, national, state, tribal, and local partners and customers

Office of Managin

Risk and Public

- Ensure that essential business functions and activities of the Department continue

Concept of Operations

- Establish reporting procedures and timeframes
- Provide reports and information as required
- Monitor status and conditions on and around key dates
- Establish appropriate coordination and command centers - Department and Bureau levels

- Place contingency locations on stand-by
- Take appropriate actions to remediate inherent Y2K problems or interruptions to business activities resulting from Y2K problems
- Test and exercise
 - Pre- and Post-

Principles

- Have sufficient information available to respond to Executive, Congressional, news media, and public inquiries
- Take remediation and response actions at the lowest appropriate management level
- Develop contingency plans for reasonable scenarios

Day One Planning Issues

- Departmental and Bureau Roles
- Information/Reporting Required
- “Command Centers”
- Testing and Exercising
- Operational Periods
- Personnel

Department-level Activities and

Responsibilities

- Receive status reports from Bureaus
- Provide status information to:
 - Departmental leadership
 - White House/CIO Council
 - FEMA
 - Congress
 - News media
 - Public
 - Employees
- Coordinate any policy or response issues requiring senior-level attention

Bureau-level Activities and Responsibilities

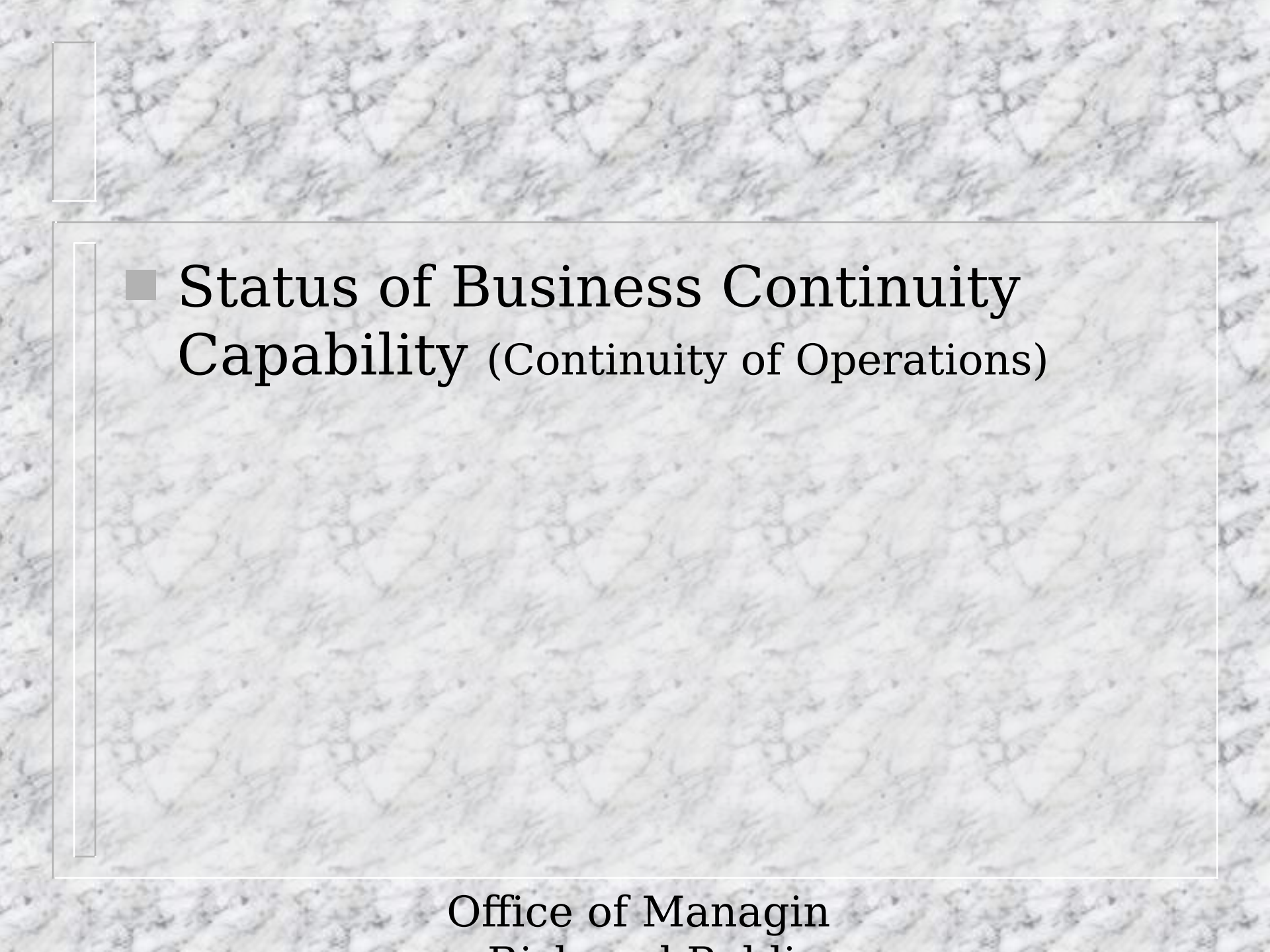
- Provide information to Department in accordance with pre-determined formats and schedules
- Perform any short-term or long-term response activities to ensure functionality of systems and equipment and continuity of essential business functions, at the lowest appropriate management level

- Support any federal government activities or initiatives to address management of consequences resulting from the transition from 1999 to 2000
- Provide information on status and any remediation/response activities to employees, contractors/partners/customers, and the public as necessary and appropriate

- Establish internal Day One procedures
- Coordinate Systems/Facilities/COO programs and information

Information Reporting to Department

- Status of Mission Critical Systems
- Status of Telecommunications Systems (Voice, Data, Radio)
- Status of Facilities and Equipment with Embedded Chips
- Status of Mission Essential and Other Important Systems



■ Status of Business Continuity Capability (Continuity of Operations)

“Command/Operations Centers”

- Department-level (Washington)
 - Ability to report on National Health of DOI
 - Coordination Department-wide information & dissemination
 - Internal dissemination of critical information
 - Problem management/problem resolution intervention as appropriate
 - Liaison with FEMA and other entities

■ Bureau Level (location at bureau discretion)

- Support Department level center
- Provide same functions within bureau as Department level center serves (coordination, problem solving support, etc.)

Proposed Operational Periods

- August 21, 1999 (times TBD)
- September 9, 1999 (times TBD)
- December 29 – 30, 1999 [specifics TBD]
- December 31, 1999 – January 1, 2000 [24 hours beginning 7 AM EST]
- January 2 - 4, 2000 – [12 hours, specifics TBD]
- January 5 - 7, 2000 – normal duty hours

Testing/Exercising

- Conduct tests of communications, reporting, and other activities prior to Operational Period
- Participate in and support tests and exercises sponsored by others

Personnel Issues

- Day One Duty Requirements - Executives, Management, Staff
 - On duty
 - On call
- Leave
 - Policy
 - Management by supervisors

- Overtime Policy
- Labor Relations Involvement
- Safety
 - Shifts
 - Rest periods

Customers

- White House/Executive Office of the President
- Congress
- FEMA
- Media/Press

Reporting Elements & Requirements

- Mission Critical Systems
- Other Systems
- Telecommunications
(Voice/Data/Radio)
- Facilities and Equipment
(Embedded Chips)
- Continuity of Operations Activity

Information/Reports for Y2K Response

- **Coordination Center**
Report on: MCS Telecommunications, Non-MCS, Facilities with Embedded Chips, Interruptions to Operations
- Timing: 8:00 EST 1/1/00, every four hours thereafter until determined otherwise
- Reports include: status, problems, consequences, fixes, time to fix, etc.

Contact Information

■ Jim Douglas

Office of Managing Risk and Public Safety
U.S. Department of the Interior

- 202-208-7963 (V)
- 202-208-5078 (F)
- jdouglas@ios.doi.gov

Office of Managin

Risk and Public

Office of Managin
Risk and Public